Protección de datos en Internet. Aplicación del reglamento

(Data protection on the Internet. Application of the regulations)

Soler Lorent, Jesús
Eusko Ikaskuntza. Miramar Jauregia. Miraconcha, 48.
20007 Donostia – San Sebastián

BIBLID [1138-8552 (2008), 20; 101-112]
Recep.: 21.07.06
Acep.: 17.10.08

La constante irrupción de las nuevas tecnologías conlleva su aplicación en todo sistema de información. En este lugar se plantea cómo se debe aplicar la protección de datos en un nuevo entorno como es Internet y en concreto la aplicación del Reglamento de Medidas de Seguridad, Real Decreto 994/1999, de 11 de junio.

Palabras Clave: Protección de datos de carácter personal en Internet. Obligatoriedad de la legislación sobre Protección de datos en Internet. Real Decreto 994/1999, de 11 de junio. Reglamento de Medidas de Seguridad. Aplicación del Reglamento de Medidas de Seguridad.

Teknologia berrien etengabeko aurrerapenak informazio-sistema osoan teknologia horiek erabiltzea ekarri du. Ildo horretan, Interneten datuen babesa nola planteatu behar den aztertzen da hemen eta, zehazki, Segurtasun Neurrien Araudiaren aplikazioa (994/1999 Errege Dekretua, ekainaren 11koa).

Giltza-Hitzak: Interneten datu pertsonalak babestea. Interneten datu pertsonalen babesari buruzko legediaren derrigorrezkotasuna. 994/1999 Errege Dekretua, ekainaren 11koa. Segurtasun Neurrien Araudia. Segurtasun Neurrien Araudiaren aplikazioa.

La constante irruption des nouvelles technologies et leur application aux systèmes d'information. Comment protéger les données dans le nouvel environnement d'Internet, par l'application notamment du Règlement des Mesures de Sécurité prévues au Décret Royal 994/1999, en date du 11 juin.

Mots Clé : Protection des données personnelles sur Internet. Application de la législation en vigueur relative à la Protection des Données sur Internet. Décret Royal 994/1999, en date du 11 juin. Règlement relatif aux Mesures de Sécurité. Application du Règlement relatif aux Mesures de Sécurité.

INTRODUCCIÓN[1]

Sobre el Reglamento de Medidas de Seguridad, Real Decreto 994/199, de 11 de junio (en adelante RMS) se debaten multitud de problemas en Cursos, Seminarios, Jornadas y Encuentros. Se debate sobre si el nivel de protección regulado en dicha normativa se otorga dependiendo del dato tratado o por el nivel del fichero declarado, si los ficheros temporales se les protege dependiendo del nivel de los datos que contienen o por el fichero matriz del que proceden, sobre la definición de fichero temporal... Son innumerables las materias sobre las que pudiera tratar la ponencia, pero por petición del equipo coordinador de estas Jornadas centraremos el objeto de debate a la aplicación del RMS en Internet.

Los compañeros de ponencia han realizado un detallado estudio de las posibilidades técnicas de las nuevas tecnologías, y dado que no es objeto de ésta reiterar los mismos conceptos, es obligado indicar dentro del título utilizado (Protección de datos en Internet) el concreto aspecto que se pretende exponer. **El supuesto del que partimos es** el estudio desde la perspectiva del RMS de una **publicación en Internet de una lista con datos de carácter personal** (DCP), habiendo obtenido previamente los consentimientos informados de todos los interesados. Es por tanto, un estudio que interesará más a prestadores de servicios o responsables de ficheros que publican datos en Internet que a los usuarios de los mismos, porque lo que está en juego es la implantación de unas medidas que suponen un desembolso económico importante en su cuantía y en su periodicidad.

Las preguntas a resolver son: ¿Se aplica el RMS a los datos publicados en Internet? y ¿quién tiene la obligación de implantar las medidas indicadas en el mismo Reglamento?

1. MARCO NORMATIVO

En primer lugar debe situarse esta nueva obligación dentro de la estructura general normativa que rige nuestras vidas, para finalmente determinar si realmente se aplican estas normas al objeto del estudio.

Con la entrada en vigor de la Ley Orgánica 15/1999, de 13 de diciembre, que traía sus orígenes del Convenio para la Protección de las personas con respecto al tratamiento automatizado de datos de carácter personal (CONVENIO 28-1-1981), de la anterior Ley Orgánica Reguladora del Tratamiento Automatizado de Datos de carácter personal (Ley 5/1992), y de la Directiva 46/95/CE, del

1. Con la entrada en vigor del Real Decreto 1720/2007 de 21 de diciembre, por el que se aprueba el Reglamento de desarrollo de la Ley Orgánica 15/1999, de 13 de diciembre, de protección de datos de carácter personal, así como la consolidación de la doctrina de Agencias, determinadas afirmaciones vertidas en este artículo deberían modificarse, pero dado que este escrito es un fiel reflejo de la ponencia expuesta en el año 2004, el artículo mantiene su interés como documento que expresa las incertidumbres jurídicas en dicho período.

Parlamento Europeo y del Consejo de 24 de octubre de 1995, (Relativa a la Protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos), se introduce una nueva filosofía en el tratamiento de los datos personales, quedando relativamente claro que el objeto de esta legislación es garantizar y proteger, en lo que concierne al tratamiento de los datos personales, las libertades públicas y los derechos fundamentales de las personas físicas, y especialmente de su honor e intimidad personal y familiar. El modo en el que se interpreta esta nueva filosofía condiciona toda la aplicación posterior de la ley.

El ámbito de protección de la ley Orgánica 15/1999 alcanza a los datos de carácter personal registrados en soporte físico, que los haga susceptibles de tratamiento, y a toda modalidad de uso posterior de estos datos por los sectores público y privado.

La propia Ley establece desde su artículo tercero la definición de dato de carácter personal y lo enuncia como cualquier información concerniente a personas físicas identificadas o identificables, indicando además que un fichero es todo conjunto organizado de datos de carácter personal, cualquiera que fuera la forma o modalidad de su creación, almacenamiento, organización y acceso. Son por tanto, unas definiciones muy amplias (la de dato personal y fichero), que abarcan prácticamente cualquier información de un individuo o aplicación informática que lo sustente.

Con la conjunción de estas definiciones podemos hacernos una idea del objeto protegido y del soporte en el que debe encontrarse los datos.

Una vez las normas indican **qué** se protege (datos personales), deben especificar **cómo** se protege. Los elementos de seguridad que deben implementarse en los sistemas de información se concretan en una serie de medidas técnicas y organizativas, siendo especificadas por lo establecido en un Reglamento (RMS).

Es por tanto, un Reglamento la norma que impone el deber de disponer de costosos sistemas de seguridad. Por eso, es necesario exponer las normas que amparan su aplicación, ya que se debe eliminar cualquier duda sobre la obligatoriedad en la aplicación del Reglamento.

En orden de jerarquía normativa, el artículo 17 de la Directiva 95/46/CE indica que:

> Artículo 17. Seguridad del tratamiento
>
> 1. Los Estados miembros establecerán la obligación del responsable del tratamiento de aplicar las medidas técnicas y de organización adecuadas, para la protección de los datos personales contra la destrucción, accidental o ilícita, la pérdida accidental y contra la alteración, la difusión o el acceso no autorizados, **en particular cuando el tratamiento incluya la transmisión de datos dentro de una red**, y contra cualquier otro tratamiento ilícito de datos personales.

Dichas medidas deberán garantizar, **habida cuenta de los conocimientos técnicos existentes y del coste de su aplicación**, un nivel de seguridad apropiado en relación con los riesgos que presente el tratamiento y con la naturaleza de los datos que deban protegerse.

En su transposición a la legislación nacional, el artículo 9 de la Ley 15/1999, de 13 de diciembre, nos indica qué acciones deben realizar los sujetos obligados por la ley:

> el Responsable de Fichero y, en su caso, el Encargado del Tratamiento, deberán adoptar las medidas técnicas y organizativas necesarias que garanticen la seguridad de los datos de carácter personal y eviten su alteración, pérdida, tratamiento o acceso no autorizado, habida cuenta del estado de la tecnología, la naturaleza de los datos almacenados y los riesgos a que están expuestos, ya provengan de la acción humana o del medio físico o natural.

Continuando con el artículo 9 de la Ley 15/1999, en su párrafo 2 y 3 se indica:

> 2. No se registrarán datos de carácter personal en ficheros que no reúnan las condiciones que se determinen por vía reglamentaria con respecto a su integridad y seguridad y a las de los centros de tratamiento, locales, equipos, sistemas y programas.
>
> 3. Reglamentariamente se establecerán los requisitos y condiciones que deban reunir los ficheros y las personas que intervengan en el tratamiento de los datos a que se refiere el artículo 7 de esta Ley.

Por lo tanto, a todas luces debe ser un reglamento el instrumento por el cual se determinen las condiciones para cumplir con esta Ley Orgánica.

Disponemos del desarrollo reglamentario, que debatido o no, sigue en vigor, desarrollado por un Real Decreto, el RD 994/1999 (RMS), de 11 de junio el cual nos especifica qué debemos disponer para cumplir con la legislación en protección de datos.

Sin carácter exhaustivo, el RMS impone una serie de obligaciones que se pueden resumir en:

Para ficheros de nivel básico debe de disponerse de:

- Un documento de seguridad
- Una definición de las funciones y obligaciones del personal
- Un registro de Incidencias
- Una relación actualizada de usuarios
- Un control de acceso
- Una correcta gestión de soportes

– Un sistema para el establecimiento de realización de copias de respaldo y recuperación

Para los ficheros de nivel medio deberá, además de lo anterior:

– Nombramiento del Responsable de Seguridad
– Realización de Auditorías periódicas
– Sistemas de Identificación y autenticación de usuarios
– Controles de acceso físico
– Sistema de gestión de soportes más complejos
– Registro de Incidencias
– Pruebas con datos reales

Para los ficheros de nivel alto, se deberá disponer de todo lo anterior más:

– Cifrado de los soportes que se distribuyan
– Registro de accesos (logs)
– Conservación de las copias de respaldo y recuperación en un lugar diferente
– La transmisión por redes de telecomunicaciones debe realizarse cifrada

Además de estas medidas, sectorizadas por niveles, existen otras normas aplicables con carácter general a todos los ficheros:

– Los ficheros temporales deberán cumplir el nivel de seguridad que les corresponda con arreglo a los criterios establecidos en el RMS.
– Las medidas de seguridad exigibles a los accesos a datos de carácter personal a través de redes de comunicaciones deberán garantizar un nivel de seguridad equivalente al correspondiente a los accesos en modo local.
– La ejecución de tratamiento de datos de carácter personal fuera de los locales de la ubicación del fichero deberá ser autorizada expresamente por el responsable del fichero y, en todo caso, deberá garantizarse el nivel de seguridad correspondiente al tipo de fichero tratado.

Todo lo indicado debe aplicarse a todo fichero que contenga datos de carácter personal, sin que la norma admita excepciones, suponiendo un esfuerzo para todo responsable de fichero que trate datos personales[2].

2. Debe hacerse patente que el legislador al crear unos textos neutros tecnológicamente, que perduren en el tiempo y que no sean influenciados por los constantes cambios tecnológicos, ha causado cierta inquietud en los sectores más técnicos no acostumbrados en frases indeterminadas de libre interpretación. Así se le ha achacado al RMS una indeterminación que impide una seguridad jurídica en su aplicación. (Como elemento de discordia recordar igualmente la Disposición Transitoria Única del RMS).

2. OBLIGATORIEDAD DE LA LEGISLACIÓN SOBRE PROTECCIÓN DE DATOS EN INTERNET

Internet ha sido el medio de transmisión de información libre por antonomasia. Parecía que se podía decir, hacer, publicar, enviar o recibir lo que se quisiera. O al menos eso era lo que se pensaba hasta la aprobación de toda una legislación reguladora del sector que se ha dictado desde hace unos años hasta fecha. Para conocer si en Internet debe aplicarse la ley Orgánica 15/1999 y sus desarrollos, debemos realizar un repaso a la legislación vigente en la materia:

Directiva 2000/31/CE, del Parlamento Europeo y del Consejo, de 8 de junio, relativa a determinados aspectos de los servicios de la sociedad de la información, en particular, el comercio electrónico en el mercado interior.

Ley 34/2002, de 11 de julio, de servicios de la sociedad de la información y de comercio electrónico:

> Artículo 1.2. Objeto: **Las disposiciones contenidas en esta Ley se entenderán sin perjuicio** de lo dispuesto en otras normas estatales o autonómicas ajenas al ámbito normativo coordinado, o que tengan como finalidad la protección de la salud y seguridad pública, incluida la salvaguarda de la defensa nacional los intereses del consumidor, el régimen tributario aplicable a los servicios de la sociedad de la información, **la protección de datos personales** y la normativa reguladora de defensa de la competencia.

Y unas extensas **Recomendaciones** que provienen **de los Grupos de Trabajo del artículo 29,** así como de **Recomendaciones de la Propia Agencia Española**

- Recomendación nº R (99) 5 del Comité de Ministros de los Estados Miembros sobre la Protección de la Intimidad en Internet, 23 de febrero de 1999, durante la 660 reunión de Delegados de Ministros.
- Grupo de Trabajo sobre protección de las personas en lo que respecta al tratamiento de datos personales. Anonimato en Internet. Recomendación 3/97, de 3.12.97.
- Grupo de Trabajo sobre protección de las personas en lo que respecta al tratamiento de datos personales. Tratamiento de datos personales en Internet. 5013/99/ES/final. WP 16.
- Grupo de Trabajo sobre protección de las personas en lo que respecta al tratamiento de datos personales. Protección de la Intimidad en el contexto de la interceptación de las telecomunicaciones. 5005/99/def. WP 18.
- Grupo de Trabajo sobre protección de las personas en lo que respecta al tratamiento de datos personales. Tratamiento de datos personales en Internet. 5085/99/ES/final. WP 25.
- WP 56 y 60 del año 2002.
- WP68 del año 2003.

– Recomendaciones a Usuarios de Internet, publicado por la AEPD desde el año 1997 y posteriormente actualizado.

En todas las referencias anteriores, se constata la aplicación en Internet de la legislación sobre protección de datos. Para confirmar esta afirmación, ya que siempre pueden quedar dudas de cómo se interpreta en su conjunto una normativa, la Sentencia del Tribunal de Justicia de la Unión Europea, de 6 noviembre de 2003, más conocida por el caso **Lindqvist**, en sus apartados 25 a 27, expone una breve explicación sobre si el tratamiento de datos personales en Internet debe considerarse un tratamiento dentro de lo que se entiende por tratamiento de Datos de Carácter Personal dentro de la Directiva 95/46/CE:

> 25.- En cuanto al concepto de "tratamiento" de dichos datos que utiliza el artículo 3, apartado 1 de la Directiva 95/46/CE, éste comprende, con arreglo a la definición del artículo 2, letra b), de dicha Directiva, "cualquier operación o conjunto de operaciones, efectuadas o no mediante procedimientos automatizados, y aplicadas a datos personales". Esta última disposición enumera varios ejemplos de tales operaciones, entre las que figura la comunicación por transmisión, la difusión o cualquier otra forma que facilite el acceso a datos. **De ello se deriva que la conducta que consiste en hacer referencia, en una página "web", a datos personales debe considerarse un tratamiento de esta índole".**
>
> 26.- Queda por determinar si dicho tratamiento está "parcial o totalmente automatizado". A este respecto, **es preciso observar que difundir información en una página "web" implica**, de acuerdo con los procedimientos técnicos e informáticos que se aplican actualmente, **publicar dicha página en un servidor**, así como realizar las operaciones necesarias para que resulte accesible a las personas que están conectadas a Internet. **Estas operaciones se efectúan, al menos en parte, de manera automatizada.**
>
> 27.- Por tanto, procede responder a la primera cuestión que la conducta que consiste en hacer referencia, en una página "web", a diversas personas y en identificarlas por su nombre o por otros medios, como su número de teléfono o información relativa a sus condiciones de trabajo y a sus aficiones, constituye un "tratamiento total o parcialmente automatizado de datos personales" en el sentido del artículo 3, apartado 1, de la Directiva 95/46".

En un ámbito más cercano, la Sentencia de la AN 28-2-2003, sobre la publicación en Internet de datos personales sin el consentimiento de los afectados (infracción del artículo 11 en relación con el artículo 44.4.b) de la Ley 1571999, indica:

> La LO 15/1999, tiene como objetivo la "protección de datos de carácter personal", denominación más amplia que la contenida en la LO 5/1992 que hablaba de "regulación del tratamiento automatizado de los datos de carácter personal". El cambio en la denominación no es anecdótico y lejos de ello se pretende, y así se desprende del articulado, dar un giro en la regulación, adecuándola a la

> Directiva 95/46 CE, conforme a la cual -art.2b)- la protección debía extenderse al tratamiento de datos de carácter personal, automatizados o no. Basta con leer el considerando 27 de la Directiva para observar como la misma indica que la protección debe aplicarse "tanto al tratamiento automático de datos como a su tratamiento manual", y que "el alcance de esta protección no debe depender, en efecto, de las técnicas utilizadas, pues lo contrario daría lugar a riesgos graves de elusión". Precisamente por ello, y entre otras cosas, en las definiciones del art.3 ya no se habla de "fichero automatizado", sino de "fichero". Debe por lo tanto entenderse que la Ley se refiere a todas las personas físicas o jurídicas, de naturaleza pública o privada, que recojan o almacenen datos en soportes físicos, sea en formato papel o en soportes informáticos, relativos a datos de carácter personal, mediante cualquier operación técnica. Debiendo entenderse por tal operación, cualquier operación, cualquier actividad o forma de recogida de datos de personas físicas, tanto la recogida manual, como la informática, por Internet o la obtenida por sofisticados medios técnicos.

La lectura sosegada de las dos anteriores sentencias tranquiliza a todos aquellos que hemos defendido que Internet no es más que un medio de trasmitir información y que por tanto, queda sometido a la normativa básica de protección de datos sin excepción. Pero, y a más a más, para corroborar lo anterior, el Director anterior de la AEPD, en su comparecencia en el Congreso de los Diputados, publicada en la Memoria de la misma Agencia en el año 2000, página 616, indicó que "la publicación vía Internet de datos de carácter personal se entiende como una cesión de datos de forma masiva".

Por último y por cerrar este argumentario que no busca más que afianzar una conclusión que tantas veces ha sido debatida, lo anterior debemos conjugarlo con las publicaciones de la Agencia Española de Protección de Datos (Memoria de la Agencia de Protección de Datos año 2000 y 2001, Atención al Ciudadano):

> En contestación a estas consultas se ha puesto de relieve que, el tratamiento de datos a través de una página Web, en principio, no se diferencia en nada de cualquier otro tratamiento y en este sentido se **le aplica en su totalidad la LOPD**.
>
> ...
>
> También se informo de que, de conformidad con el Reglamento aprobado por Real Decreto 994/1999, de 11 de junio (BOE 25-6-1999) deberán de redactar el documento de seguridad regulado en el artículo 8 del referido Reglamento y **adaptar las medidas de nivel básico, medio o alto que correspondan**. Dicho documento no tiene que ser presentado en la Agencia, sino tan sólo tenerlo disponible por si les fuera requerido.

Por lo tanto, y sin género de duda, **podemos concluir que los datos personales publicados en Internet deben ser protegidos de igual forma que los datos tratados en modo local.**

3. APLICACIÓN DEL REAL DECRETO 994/1999

En los apartados anteriores se ha pretendido convencer a los más escépticos sobre la obligatoriedad de cumplir con todo lo indicado en la normativa de protección de datos en los supuestos de tratamiento de datos personales en Internet, pero ¿la realidad es tan estricta?

No hay nada mejor que mostrar la actitud de la Agencia Española de Protección de Datos respecto a cómo entiende la aplicación del RMS en Internet con parte de una resolución sancionadora de la propia Agencia sobre esta materia.

La Memoria de la AEPD del año 2002, en su apartado "El uso de Internet y la protección de datos personales: los sistemas de autenticación on-line" contiene una sección completa sobre las "Medidas de seguridad en el acceso a ficheros automatizados con datos de carácter personal" e indica:

> De las actuaciones previas realizadas por la Inspección de Datos se pudo concluir que, como consecuencia de una avería en el sistema informático en el que se ubicaba el fichero automatizado con la información relativa a las órdenes de instalación del servicio de acceso a Internet, combinada con un deficiente funcionamiento de los sistemas definidos para la realización de copias de respaldo y recuperación de datos, se tuvo que optar, por parte de la entidad responsable, por realizar un procedimiento de recuperación que tuvo como consecuencia la aparición de una vía alternativa de acceso a la información. Esta alternativa carecía de un control de acceso en las condiciones de seguridad establecidas de forma habitual. Como consecuencia de ello se produjeron accesos a datos personales de los clientes de servicio por parte de personas que no eran usuarios autorizados del sistema, accesos que no pudieron ser evitados por los mecanismos existentes.

Continúa la memoria recogiendo las alegaciones de la empresa sancionada, indicando:

> La imputada, en sus alegaciones, manifestó que los accesos se produjeron motivados por una situación imprevisible y con una absoluta carencia de intencionalidad por su parte, señalando además que dichos hechos únicamente podían haber sido ejecutados tras una búsqueda de puntos débiles en sus sistemas de seguridad que en ningún momento podían tener un objetivo lícito. Reforzaba su argumentación haciendo constar que los responsables de los accesos en ningún momento se habían puesto en contacto con ellos para advertirles de dicha posibilidad, si bien aprovecharon el intervalo temporal en que fue posible para la descarga de ficheros cuya titularidad no les correspondía.

Frente a dichas alegaciones, en la resolución del procedimiento sancionador se vierten diversas precisiones al respecto basadas en lo establecido en el Reglamento de Medidas de Seguridad.

> Dicha norma establece una serie de medidas que, en su conjunto, proporcionan un determinado nivel de seguridad, siendo determinante la idea del conjunto puesto que la presencia de debilidades en alguna de las medidas puede hacer

> inútiles las otras por muy robusta que sea su definición e implementación. De aquí que en la literatura especializada se considere el concepto de arquitectura de seguridad como referido a un conjunto integrado e interdependiente de reglas de servicio en contraposición al concepto de una serie de medidas aisladas e independientes entre sí. En este sentido, y en lo que tiene que ver con los sistemas de información, la arquitectura.

Sigue en las páginas siguientes argumentando la aplicación del artículo 12 y 14 del RMS y por tanto se sanciona por incumplimiento del artículo 9 de la LOPD

A todo esto, que como dice la propia AEPD (páginas 201):

> se alegó, por parte de la entidad imputada, la involuntariedad en el hecho que causó el error del sistema que está en el origen de los envíos, la pronta corrección del mismo una vez detectado y la ausencia de perjuicio para los afectados. Además, se cuestionaba en dichas alegaciones el carácter de dato personal de la dirección de correo electrónico. La resolución del procedimiento, rebate la consideración de la falta de culpabilidad como eximente de sanción alegada por la entidad, con el argumento de que si bien ese tipo de conductas no tienen «per se» un carácter doloso, y en la mayoría de los casos presentan una falta de intencionalidad, basta con la simple negligencia en el cumplimiento de los deberes impuestos por la Ley a los responsables de los ficheros para que estas conductas puedan ser objeto de sanción conforme a lo establecido en la LOPD.

Con esta resolución queda patente la posición de la Agencia Española de Protección de datos de aplicar el RMS también a los datos publicados en Internet, además de aplicarlo de una forma extremadamente rigurosa. Por tanto, deben aplicarse **todas** las medidas establecidas en el RMS.

4. REFLEXIONES SOBRE LA APLICABILIDAD DEL RMS

Todo lo expuesto puede causar la sensación de estar frente a una normativa excesivamente mecanicista en su aplicación y que poco espacio deja para la interpretación. Nada más lejos de la realidad. Existen multitud de aspectos que quedan abiertos a la discusión, ya que el mundo virtual genera gran cantidad de incógnitas, y entre ellas, a modo de reflexión presentamos las que siguen:

4.1. Sobre los encargados de tratamiento

Si la información publicada en la red se encuentra en servidores de otros (de un encargado de tratamiento) las medidas de seguridad que debe implementar el Responsable del Fichero serán todas la indicadas en el RMS, las cuales, parte o su conjunto, podrá trasladárselas al Encargado de Tratamiento. En todo caso este traslado de obligaciones deberá ser indicado en el contrato correspondiente cumpliendo las cláusulas del artículo 12 de la Ley 15/1999, "obligándose a que figure **detallado** de forma explícita el conjunto de instrucciones del respon-

sable del fichero al tercero responsable del tratamiento a realizar" (página 204 Memoria del año 2002 de la AEPD).

Si el encargado de tratamiento es el obligado a aplicar todas las medidas de seguridad, tal y como indica el artículo 9 de la Ley 15/1999, será éste el que debe implantarlas. Planteando una duda. Si este encargado realiza una mera función de hospedaje, no conociendo el tipo de datos que maneja, ¿debe aplicar todas las medidas de nivel alto por defecto? o ¿debe redactar tres servicios tipo equiparables a los niveles de seguridad?

En principio, parece más sencilla la segunda posibilidad, redactar tres o más contratos tipo de servicios, comprometiéndose los clientes a no modificar el nivel de los datos utilizados o a novar el contrato en caso contrario, responsabilizándose en caso de modificación sin notificación.

4.2. Cancelación de datos en internet

Mayor problema supondrá el supuesto de ejercicio del derecho de cancelación de un dato. Incluso en el supuesto de disponer del consentimiento de los afectados para tratar sus datos personales, aún habiendo informado de todos los requisitos establecidos en el artículo 5 de la Ley 15/1999, la cancelación de un dato puede generar mayores problemas que la publicación del dato. La Agencia Española de Protección de Datos en su Memoria del año 2001 en respuesta a una consulta que se le formulaba sobre la supresión o cancelación de un dato, indicaba que los datos deben ser cancelados, posteriormente bloqueados y finalmente suprimidos.

En este mismo sentido, una sentencia de la Audiencia Nacional (Sala de lo Contencioso-Administrativo, Sección 1º), de 14 de septiembre de 2001, en su Fundamento de Derecho Cuarto, último párrafo, indica que

> el titular del fichero debe proceder a la cancelación del dato en todos los soportes que posea; de forma tal que el dato desaparezca de todo soporte informático dependiente del titular del fichero.

Si tal y como hemos indicado, un Responsable de Fichero debe implementar todas las medidas de seguridad, y entre las mismas se encuentra realizar las correspondientes copias de seguridad, debe cancelar dicho dato en todas las copias de respaldo.

Si añadimos la figura anteriormente comentada de Encargado de tratamiento que almacena multitud de páginas web o ficheros con datos personales de otros Responsables de Fichero albergándolos en un mismo servidor, y sobre el cual ha realizado copias de respaldo en su conjunto (no diferenciando ficheros) en períodos mínimos semanales, tiene la obligación de hacer desaparecer **un sólo dato** de todas las copias de respaldo guardadas.

Para la jurisprudencia, como para la Agencia, parece obvia esta interpretación. Desde el punto de vista técnico, realizar esta labor es altamente costoso.

4.3. Ámbito de aplicación de las medidas de seguridad

Tal y como indica el artículo 5 del RMS las medidas de seguridad exigibles a los accesos a datos de carácter personal a través de redes de comunicaciones deberán garantizar un nivel de seguridad equivalente al correspondiente a los accesos en modo local. Debe determinarse si la publicación de datos en Internet supone una cesión masiva de datos (manifestado por el Director de la Agencia Española en el Congreso) o por el contrario tal publicación no es una cesión, sino el acceso por un usuario "Sujeto o proceso autorizado para acceder a datos o recurso. Artículo 2 del RMS" en un terminal.

La aceptación de una cesión masiva de datos supondría que el Responsable del fichero no debe garantizar las medidas de seguridad una vez que se produzca la efectiva cesión, siendo obligación del cesionario implementar las mismas a su costa. Si por el contrario, la visualización no se entiende como cesión sino como un acceso por un usuario, el Responsable de Fichero debe garantizar todas las medidas de seguridad en el equipo de usuario.

Técnicamente el segundo supuesto es inviable: ¿Puede el Responsable de fichero garantizar que el terminal de un usuario de cualquier parte del mundo dispone de las medidas de seguridad establecidas por el RMS?

Por otra parte, la primera solución impone al cesionario (cualquier persona que navegue por Internet) la obligación de implementar todas las medidas del RMS por visualizar dichos datos, a no ser que mantenga dicho fichero una persona física en el ejercicio de actividades exclusivamente personales o domesticas (artículo 2.2.a) de la Ley 15/1999). Pensemos en la cantidad de accesos a Internet que se realizan desde puestos de trabajo.

Es por tanto indispensable determinar hasta dónde llega la responsabilidad de implantar el RMS al visualizar datos en Internet.

5. CONCLUSIÓN

El legislador ha realizado un enorme esfuerzo por proteger los derechos fundamentales de las personas físicas en cuanto al tratamiento de sus datos personales creando una legislación garantista que olvida al Responsable del Fichero o a las personas que deben implementar las medidas técnicas que hacen posible cumplir con la legislación.

El RMS, que desde el punto de vista jurídico nace como el desarrollo de una ley, genera en su aplicación tales problemas interpretativos que no debe ser olvidado ni relegado a un segundo plano por su carácter técnico y de aplicación por los informáticos, ya que su implantación puede generar enormes costes para las organizaciones y la sociedad.